Chapter 47
SVM-Based Traffic Data Classification for Secured IoT-Based Road Signaling System

Suresh Sankaranarayanan
https://orcid.org/0000-0001-5145-510X
SRM Institute of Science and Technology, Chennai, India

Srijanee Mookherji
SRM Institute of Science and Technology, Chennai, India

ABSTRACT

The traffic controlling systems at present are microcontroller-based, which is semi-automatic in nature where time is the only parameter that is considered. With the introduction of IoT in traffic signaling systems, research is being done considering density as a parameter for automating the traffic signaling system and regulate traffic dynamically. Security is a concern when sensitive data of great volume is being transmitted wirelessly. Security protocols that have been implemented for IoT networks can protect the system against attacks and are purely based on standard cryptosystem. They cannot handle heterogeneous data type. To prevent the issues on security protocols, the authors have implemented SVM machine learning algorithm for analyzing the traffic data pattern and detect anomalies. The SVM implementation has been done for the UK traffic data set between 2011-2016 for three cities. The implementation been carried out in Raspberry Pi3 processor functioning as an edge router and SVM machine learning algorithm using Python Scikit Libraries.

1. INTRODUCTION

Traffic Congestion is a very perennial problem in many countries. India which is a developing country is no exception to this.

DOI: 10.4018/978-1-7998-7705-9.ch047

Internet of Things (IoT) (Li et al, 2016; Sakran and Hasan, 2015; Mone et al, 2015; Zhiguang et al, 2017) is slowly and steadily becoming a part of almost every technology. IoT in transportation system can assist in integration of communications, control, and information processing.

IoT architecture as such is widely distributed into three layers which are the perception layer, the network layer and the application layer (Abomhara and Geir, 2014; Granjal et al, 2015). These layers are susceptible to various security threats and attacks. The attacks that the systems are vulnerable to are the denial of service attack, the DY intruder attack and privacy attacks like eavesdropping, traffic analysis and finally data mining. Along with these common attacks, there are many more vulnerabilities present in each layer that can lead to many more recent and common attacks along with various zero-day vulnerability attacks.

Lot of IoT security protocols (Shanmugavadivu and Nagarajan, 2011; Sinha et al, 2013) have been suggested and many frameworks have also been researched upon that involves the use of IDPS in an IoT network to detect and block any incoming attacks from an end device. But none of these systems are intelligent or smart enough in detecting the attacks or anomalies in IoT where data are heterogeneous in nature.

There has been research done with machine learning techniques in a normal network in general (Hammer et al, 2015; Rathore and Sushmita, 2013; Singh and Nidhi, 2014; Buczak and Erhan, 2016). The work till date has been achieved to a level of automatically labeling data by studying its content and classifying into various security classes.

Now in terms of securing an IoT based Traffic Signaling by employing Machine Learning, there has been no research work reported till date. So, based on the security issues and challenges in IoT based Traffic Signaling system, security is much of a concern at the edge level where all analytics carried out for regulating the traffic.

In IoT, data are heterogeneous in nature and this requires machine level intelligence in defending against attacks based on data pattern. The standard security protocol or cryptosystem are not effective in case of heterogeneous data in IoT system. So, towards this machine learning would play a vital role in defending against anomalies.

So accordingly, we here have developed a security classifier system at the Edge called Fog computing or Edge computing node by employing Support Vector machine learning algorithm for classifying the data as good or bad (Srijanee and Suresh, 2018). Standard security protocols cannot be very effective in IoT based Traffic Signaling system as traffic data being generated are heterogeneous in nature and varies a lot from region to region.

The machine learning at the Edge which here is Raspberry Pi3 would train the system based on traffic data set against Man in Middle attack in IoT system.

The system based on training would predict incoming traffic data from IoT device as good or bad (Srijanee and Suresh, 2018). The system based on SVM classifier also been evaluated for accuracy of prediction which has resulted in an effective system. The SVM machine learning been implemented in Edge node which is Pi3 for UK Traffic data set (Traffic Data, n.d) for five years for three cities which are Merton, Harrow and Hillingdon using Sklearn.

The rest of paper is organized as follows. Section II gives a complete literature Review on Security in IoT system followed by Machine learning in Information security and IoT in Intelligent Transport System. Section III gives system architecture, System design and Pseudo code algorithm for implementation of SVM in security analysis for Traffic Data. Section IV talks on implementation details of SVM in Pi3 with accuracy of prediction and validation of system. Section V gives the conclusion and Future work.